by JERRY CORBIN

A Fuzzy Logic-Based Financial Transaction System

An ATM's digital safeguards depend on analog information-gathering techniques. One of the best ways to improve on magnetic stripe precision is through the use of fuzzy logic.

Rupert Adley

In the early days of credit cards, fighting fraud was as simple as issuing a weekly bulletin listing the numbers of lost or stolen cards. But as the credit card market has grown, so has the sophistication of crooks to bilk merchants, card issuers, and consumers out of millions of dollars. Card fraud is a big business, and criminals are finding ways to circumvent the industry's most sophisticated security measures.

Experts estimate that in 1993, the total credit card fraud loss in the U.S. ran close to a billion dollars, up from $864 million in 1992.[1] One of the fastest growing types of fraud involves counterfeiting valid cards. MasterCard International reportedly lost $113 million in 1993 to card counterfeiting, and Visa International is reported to have lost roughly $160 million to card counterfeiting in the same period.

Counterfeiting also costs consumers millions of dollars each year. By law, if the card issuer determines that the customer has been defrauded, the victim is not liable for losses over $50. In many cases, the issuer may simply eat the $50. But in some cases, the card issuer may refuse to cover the loss on the grounds of insufficient proof of fraud.

Card issuers have taken steps to thwart card counterfeiting. Holograms were introduced in the 1980s to make cards harder to copy. Unfortunately, counterfeiters are now able to make such close replicas of valid cards that it's virtually impossible for a store clerk to tell if a particular card is legitimate. Joel Lisker, vice president of security and risk management at MasterCard, is reported to have said,

Despite all the hype about smart cards, magnetic stripe-based cards will be around for a long while yet.

"The quality of Chinese counterfeiting is so good that only experts can tell the difference between a genuine and simulated hologram."[2]

IMPROVING SECURITY

Recently, card issuers have started adding new, hard-to-copy codes to the magnetic stripe to make counterfeiting more difficult. The code uses a secret algorithm to generate a three-digit number based on the account number and expiration date. This secret value is then encoded onto the magnetic stripe of a new card. Knowing the account number and expiration date is not enough information for a crook to successfully counterfeit a valid card; a counterfeiter would also have to know the mathematical algorithm.

MasterCard calls this code the Card Validation Code (CVC), and Visa calls its version Card Verification Value (CVV). Unfortunately, many retail outlets have not upgraded their credit card verification code scanners to accurately check valid codes. MasterCard and Visa require new card issuers to include this code on the magnetic stripe of newly issued credit cards and are encouraging merchants to update their credit card verification scanners.

In the Asia-Pacific region, a hotbed of credit card counterfeiting, the introduction of CVC and CVV has cut MasterCard's and Visa's losses somewhat. Card companies know they can't afford to let down their guard and that it's only a matter of time before they'll need newer, more sophisticated weapons against card counterfeiting.

Also, the new codes do nothing to thwart card "skimming," a fast-growing form of card counterfeiting in which a valid card is obtained and the counterfeiter copies or skims all the information from the magnetic stripe, including the new hard-to-copy codes. "We think (the code) is an interim stand-in measure," Visa senior vice president Steve Ruwe is quoted as saying. "It doesn't deal with skimming."

Some concepts being explored to improve the security of credit cards include "smart cards," which contain computer chips with non-volatile memory (usually EEPROM) and some intelligence in the form of a small microcontroller or specialized logic to secure the information contained in the memory and other intelligent features.

Smart cards have received much press coverage despite the fact that magnetic stripe-based cards are used more often than smart cards by several orders of magnitude. Smart cards are being touted (particularly in Europe) as the answer to the industrialized world's march towards a cashless society. Smart cards are envisioned as being the solution for enhanced security, as well as providing additional intelligent features for credit cards, debit cards, telephone charge cards, bank ATM cards, and a wide variety of other applications. It is not clear yet exactly what intelligent features consumers will desire from smart cards.

Despite all the hype about smart cards, magnetic stripe-based cards will be around for a long while yet. For one thing, there is a huge installed base of magnetic stripe credit card readers at the merchant locations. To phase this installed base over to smart card readers would be a tremendously expensive venture. And the cost of smart cards is roughly an order of magnitude more than the cost of magnetic stripe-based cards. Banks and new card issuers will not make the decision to change over from magnetic stripe-based cards to smart chip cards unless consumer demand for new intelligent features (beyond enhanced security) is strong enough to justify the huge expense.

This may not happen anytime soon.

One company, XTec Inc., has designed a magnetic stripe-based card system called XSec that answers many security concerns and compares very favorably with smart cards in many respects.[3] The company is engaging its fuzzy logic-based system with card companies, banks, vending machine distributors, and people interested in a secure magnetic stripe card system.

FUZZY LOGIC-BASED SYSTEM

The XSec system uses the natural magnetic "jitter" of the data encoded on the magnetic stripe of a card to verify its authenticity. Jitter is present on any magnetically encoded card, and every card stripe is physically different. The signature of the card is determined every time the card is read and is compared with the original signature value. The signature value will be the same if the card is genuine. A counterfeit card will produce a different signature. The original signature may be stored on the card, or online in the system. The system effectively thwarts card counterfeiting, including skimming, since the signature of each magnetic stripe card is unique.

Most credit card readers on the market use integral detectors for reading data. The biggest problem with integral detectors is that they are sensitive to wear and degradation of the magnetic stripe, which affects the read reliability of integral readers. Many professionals in magnetic stripe technology believe that jitter is a variable and serious problem in magnetic stripe reading. However, when true peak detectors are used, this criticism is not valid. True peak detectors are being used more frequently in readers designed to read magnetic cards with a greater degree of reliability than conventional readers.

In a true peak detector, only the position of the peak of the voltage waveform from the magnetic head is used for decoding. This corresponds to the zero crossing of the flux of the magnetic card. This position is very stable and insensitive to wear and damage. The peak position measurement is therefore a very reliable method for reading and securing cards.

In this system, jitter is measured to a precision of better than 0.5% by means of simple inexpensive digital techniques. Jitter as small as 1% allows reliable security for any card.

To determine the data decoding security characteristic for a card, the reader measures the intervals between flux reversals on the card, which correspond to the peak of the voltage waveform from the magnetic head, as shown in Figure 1. Data from the interval measurements is used to determine the security characteristic of the card.

If any data is damaged or missing from the card, it can be reconstructed by digital data processing with the error-correcting codes already on the card, significantly enhancing card reliability. Conventional readers have great difficulty reconstructing lost data.

The system also utilizes some proprietary techniques that further improve the read reliability of cards.

Lost or damaged data and read-induced errors do not affect the security reliability, since fuzzy logic techniques are used in security key determination and subsequent card authentication. Such fuzzy logic techniques allow some differences between individual card reads. If some of the events of the "fuzzy data set" are not the same, the card may be authenticated, provided most of the events in the fuzzy data set are the same. Table 1 shows some fuzzy data sets for the same card read multiple times at different points in a field trial of the system. This magnetic stripe card system compares favorably with smart card approaches in several important areas, as shown in Table 2.

WHY FUZZY LOGIC?

In effect, this application is a pattern recognition type of application that uses the magnetic jitter patterns of a magnetic stripe to form a signature for the stripe. The signature is made up of a fuzzy data set. Fuzzy logic is particularly well suited for this type of application.

First, fuzzy logic software allows the use of a low-cost, high-performance 8-bit microcontroller such as Microchip's PIC17C42, which offers the execution throughput, peripheral features, and software code protection necessary for this application. A more mathematically intensive approach

FIGURE 1

Time interval measurements between adjacent flux transactions.

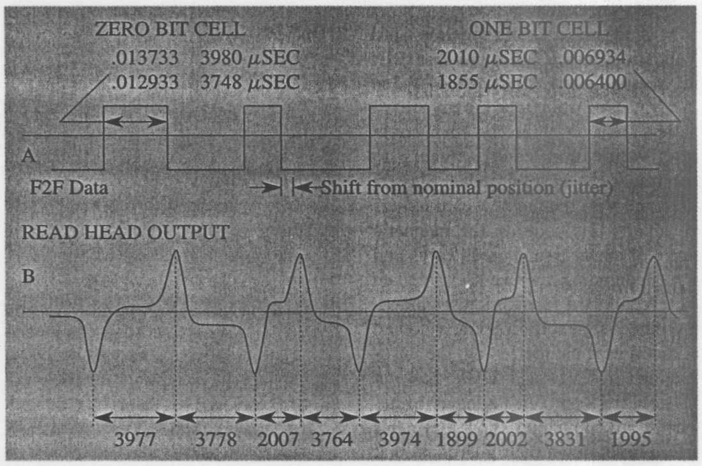


TABLE 1
Normal fuzzy data set.

Date	Time	Fuzzy Set
6/17/93	15:39:01	04 03 12 0F 05 03 03 01 0A 01 00 00 07 0D 01 05 05 21 0D 05 FF 0D 0D 01 0F 0B 08 01 04 04 01 0C
6/19/93	9:12:03	04 03 0A 0F 05 03 03 01 0A 01 00 00 07 0D 01 05 05 21 0D 03 FF 0D 15 09 17 13 08 01 04 04 01 0C
6/26/93	11:23:22	04 03 1A 0F 05 03 03 01 05 01 00 08 07 0D 01 05 05 21 15 03 07 0D 15 09 0F 13 08 01 04 04 01 0C
6/28/93	13:15:19	04 03 1A 0F 05 03 03 01 0A 01 00 08 07 0D 01 05 05 19 15 03 07 0D 15 09 0F 13 08 01 04 04 01 0C
7/2/93	16:11:22	04 03 0A 0F 05 03 03 01 02 01 00 00 07 0D 01 05 05 21 0D 03 FF 05 15 09 0F 0B 08 01 04 04 01 04
7/10/93	18:40:14	04 03 0A 0F 05 03 03 01 0A 01 00 00 07 0D 01 05 05 19 0D 03 07 0D 15 09 0F 0B 10 01 04 0C 06 0C
7/16/93	17:26:23	04 03 0A 0F 05 03 03 01 0A 01 00 00 07 0D 01 05 05 19 15 15 07 0D 15 09 07 0B 08 01 04 04 01 0C
7/17/93	8:52:04	04 03 0A 01 05 03 03 01 05 01 03 08 07 15 01 05 0D21 15 15 07 0D 1D 09 0F 13 08 01 04 0C 01 0C
7/26/93	19:53:31	04 03 0A 07 05 03 03 01 02 01 00 00 07 0D 01 05 05 19 0D 05 07 0D 15 09 0F 0B 08 01 04 04 01 0C
7/29/93	19:50:50	04 03 12 07 05 03 03 01 0A 01 00 00 07 0D 01 05 05 21 15 0D07 0D 15 09 17 13 10 01 04 04 01 0C

based on complex statistical analysis would require a much more expensive processor or DSP. Because the fuzzy logic algorithm is considerably shorter and simpler than other approaches, the performance of the 8-bit microcontroller is more than adequate to provide real-time card reading control and fuzzy logic card authentication.

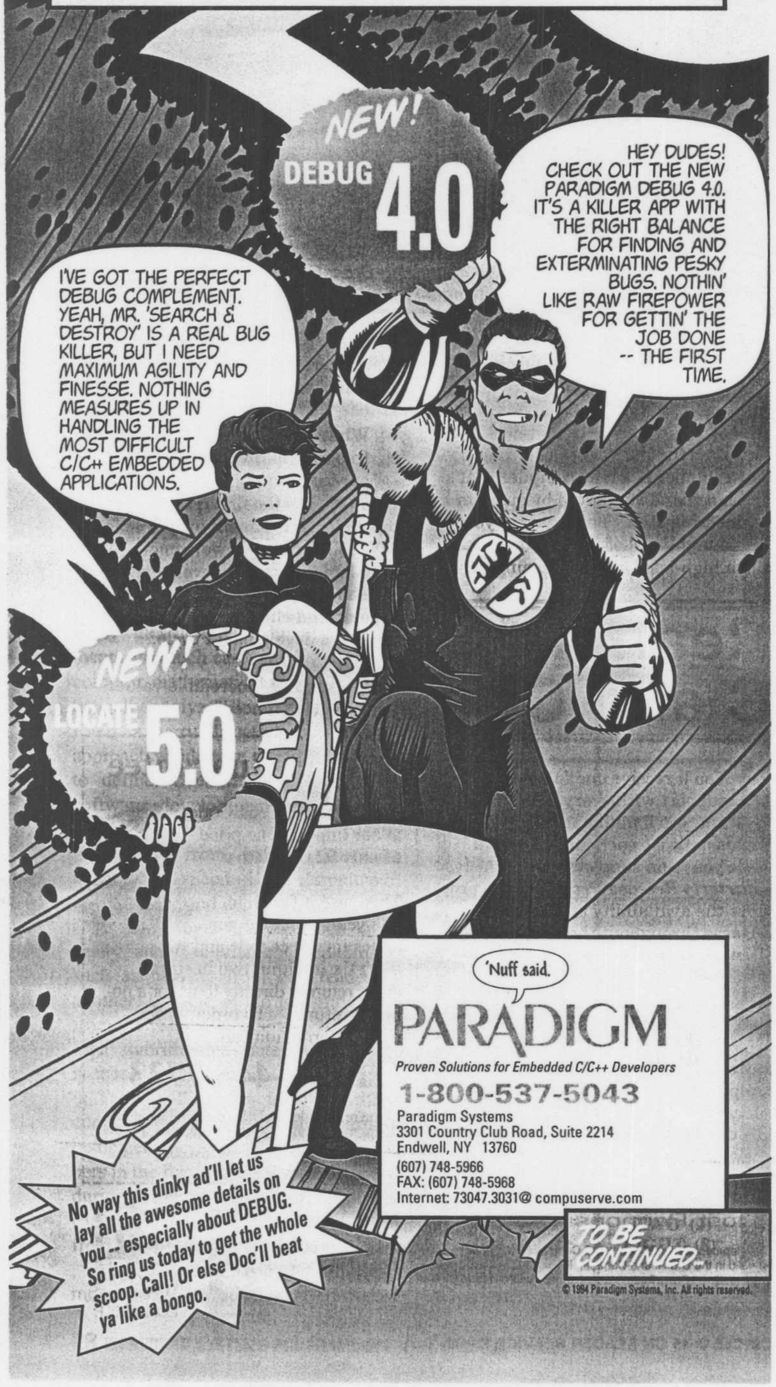
Fuzzy logic dramatically shortens the system development time since membership functions and a set of fuzzy rules defined as linguistic statements are much easier to define than a complex mathematical model that statistically analyzes the magnetic stripe. Even a very large look-up table approach would take considerable time to define. User-friendly fuzzy logic software development tools with a graphical interface, such as fuzzyTECH-MP from Inform Software Corp., can speed fuzzy logic code development and debugging.

A fuzzy logic approach can more easily adapt to changing conditions such as moving from one reader to another. If some of the incoming data from the readers is incorrect, the fuzzy logic algorithm may determine correctly that a card is genuine. For example, in Table 1, the fuzzy logic algorithm correctly recognized the same card as being genuine, even though some numbers in the fuzzy data set were different during different readings. Fuzzy logic can more naturally handle variations from the magnetic stripe readers.

Also, the fuzzy logic algorithm can more easily be adapted to different

TABLE 2
Comparison of magnetic stripe cards to smart cards.

Requirements for Transaction Cards of the Future	Standard Stripe		Chip Card		XSEC	
Compatibility	Existing technology	+	Requires all new technology	-	Fully compatible with existing & new technology	+
Capabilty	Online only	-	Online & stand-alone	+	Online & stand-alone	+
Fraud Resistance	Easy to alter or copy	-	Difficult to alter or copy	+	Difficult to alter or copy	+
Versatility	Charge card Debit card	-	Charger card Debit card Cash card EBT	+	Charger card Debit card Cash card EBT	+
Card Life	Two years	-	Unknown	-	More than two years	+
Immunity to Environmental Hazard	Magnetically volatile	-	Electrostatically volatile	-	Magnetically & Electrostatically volatile	+
Low Cost	Card cost < $0.50	+	Card cost < $5.00	-	Card cost < $0.50	+
Transaction Cost	High	-	Low	+	Low	+
Storage Capacity	119 Characters (Tracks I & II)	-	4 K Bytes (excessive capacity leads to excessive cost)	-	375 Characters (Tracks I, II & III)	+
Stored Value Capacity	Impractical	-	Incrementing & decrementing value	+	Incrementing & decrementing value	+
Bottom Line	**TWO (2)** **EIGHT (8)**	+ -	**FIVE (5)** **FIVE (5)**	+ -	**TEN (10)**	+



cards for different applications. Credit cards, debit cards, security entrance cards, bank ATM cards, and train and subway cards could use variations on basically the same fuzzy logic algorithm. The time and cost to modify the fuzzy logic algorithm is not large compared to other approaches.

Fuzzy logic can be used effectively to reconstruct lost data. With the XSec system, even severely scratched magnetic stripes can be read and used. To accomplish this using other more math-intensive statistical analysis would be much more difficult.

In this article, we reviewed the problem of credit card security and explored some of the actions credit card companies have taken to reduce credit card fraud. We described an enhanced magnetic stripe-based system based on fuzzy logic that dramatically improves the security of magnetic stripe cards. We compared this system to smart cards and found that the enhanced magnetic stripe card system offers enhanced card security and some other advantages of the smart cards at a much lower cost. Finally, we learned that fuzzy logic is particularly well suited for this type of pattern-recognition application, and it can dramatically ease the system development process. ESP

Jerry Corbin has worked in the microprocessor and microcontroller marketing field for 15 years. He joined Microchip Technology Inc. in 1993 as a product marketing manager for the PIC16/17 family of microcontrollers. Corbin has a BS in physics and an MBA from Ohio State University.

REFERENCES

1. Holland, Kelly, "Stalking the Credit-Card Scamsters," *Business Week*, Jan. 17, 1994, pp. 68-69.

2. Punch, Linda, "Battling Credit Card Fraud," *Bank Management*, March 1993, pp. 18-20.

3. Jeffreys, Denise. *The Future of Magnetic Stripe Technology*. Miami, FL: XTec Inc., Oct. 13, 1993.